POWERED BY Dialog

F1

Signal key coding method for vehicle security application - generating random code and performing message interrogation with transponder forming response from message and encryption key

Patent Assignee: VALEO ELECTRONIQUE
Inventors: BOSCHINI A

Patent Family

Patent Number	Kind	Date	Application Number	Kind	Date	Week	Type
FR 2717327	A1	19950915	FR 942919	A	19940314	199542	B

Priority Applications (Number Kind Date): FR 942919 A (19940314)

Patent Details

Patent	Kind	Language	Page	Main IPC	Filing Notes
FR 2717327	A1		30	H04B-007/14	

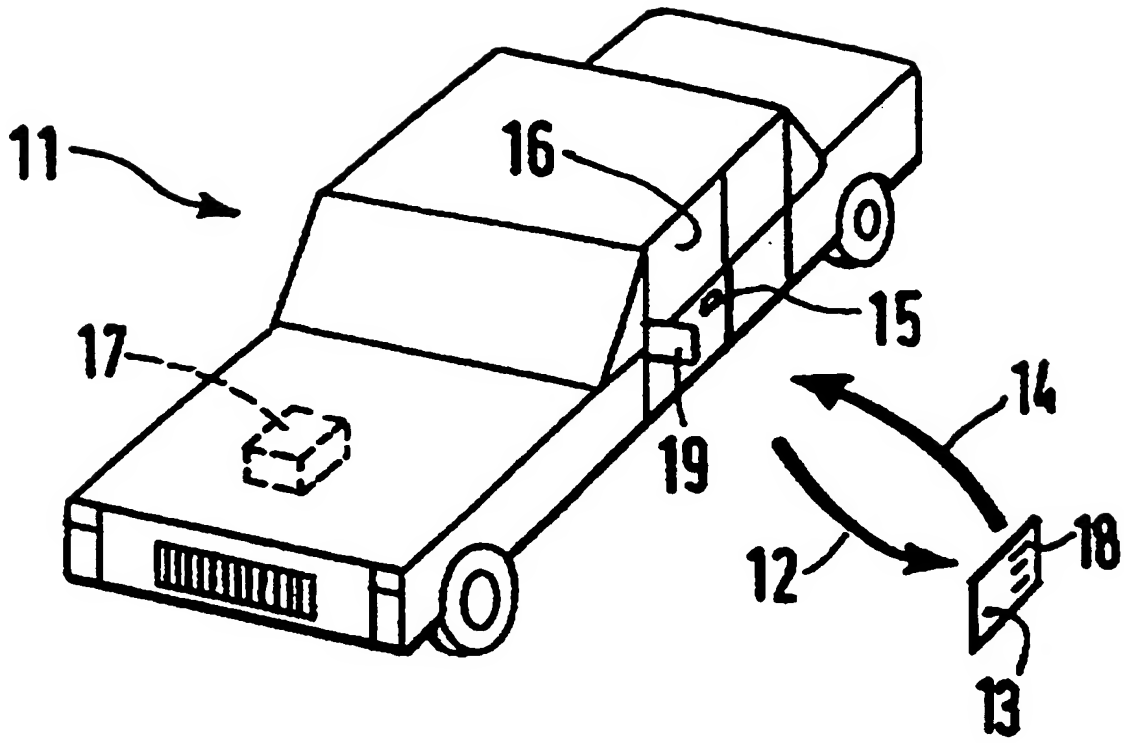
Abstract:
FR 2717327 A

The method involves an interrogator (17) used by the owner generate a random signal and form an interrogation message. The transmission is sent to a transponder (13) in a vehicle (11). The transponder receives the messages, and calculates a response. The response is a function of the random code and an encryption key.

The message response is formed and sent back to the interrogator. The interrogator calculates the expected response, and on reception carries out a comparison. The interrogator identifies if the key is correct.

ADVANTAGE - Does not need write stage so EEPROM is not required. High speed operation. Low cost, flexible and compact. Durable.

Dwg.1/5



Derwent World Patents Index

Dialog® File Number 351 Accession Number 10421232

F1

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 717 327**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **94 02919**

(51) Int Cl° : H 04 B 7/14

(12) DEMANDE DE BREVET D'INVENTION 30 A1

(22) Date de dépôt : 14.03.94.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : 15.09.95 Bulletin 95/37.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule.*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *VALEO ELECTRONIQUE - Forme Juridique : Société Anonyme* — FR.

(72) Inventeur(s) : Boschini Alain.

(73) Titulaire(s) :

(74) Mandataire : Valéo Management Services.

(54) Procédé de communication entre un module d'interrogation et un transpondeur utilisé en particulier pour le déverrouillage des ouvrants et/ou des immobiliseurs d'un véhicule, et dispositif d'identification le mettant en œuvre.

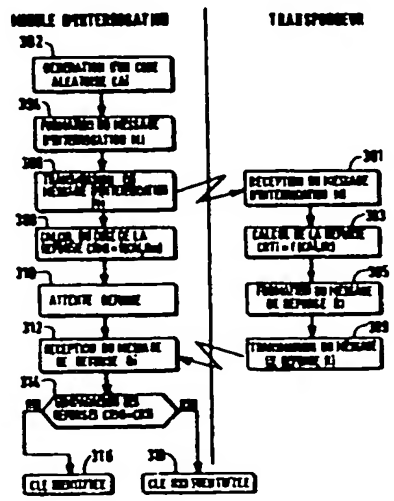
(57) Procédé de communication entre un module d'interrogation et une clé à transpondeur, utilisé pour le déverrouillage des ouvrants et/ou des immobiliseurs d'un véhicule automobile, du type comportant une séquence d'identification consistant:

- à interroger la clé en émettant au moins un signal d'interrogation contenant un code aléatoire CAI,
- à calculer le code de réponse attendu (CRMI) par le module d'interrogation suivant la fonction CRMI=f(CAI, Km) où Km est une clé de cryptage,
- et à le comparer avec un code de réponse de la clé transpondeur (CRTI) reçu, celui-ci étant calculé par un processeur du transpondeur suivant la fonction CRTI=f (CAI, Kt) où Kt est une clé de cryptage propre au transpondeur.

Compte tenu de la propriété d'injectivité de la fonction de cryptage (f):

- si le code de réponse du transpondeur (CRTI) et le code de réponse attendu (CRTI) sont égaux, il y a identification de la clé,
- sinon il y a non identification;

Dispositif de télécommande mettant en œuvre un tel procédé.



FR 2 717 327 - A1

REPUBLIQUE FRANÇAISE

2717327

INSTITUT NATIONAL de la PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 493594
FR 9402919

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée de la demande examinée
X	US-A-4 680 036 (HIRANO,TAKEUCHI,NAKANO) * colonne 3, ligne 7 - colonne 4, ligne 26; figure 1 *	1,12
A	EP-A-0 284 133 (T.R.T) * colonne 2, ligne 42 - colonne 4, ligne 38; figures 1,2 *	1-4,6
A	COMPUTERS & SECURITY, vol.11, no.2, 1 Avril 1992, OXFORD pages 173 - 183 ROTRAUT LAUN 'asymmetric user authentication'	1-4,6

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.5)

E05B
H04L

Date d'achèvement de la recherche: 23 Septembre 1994

Examinateur: Herbelet, J.C.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

La présente invention concerne un procédé de communication entre un module d'interrogation et un transpondeur utilisé en particulier pour le déverrouillage des ouvrants et/ou des immobiliseurs d'un véhicule, et un dispositif d'identification mettant en oeuvre un tel procédé.

L'invention s'applique plus particulièrement aux systèmes d'identification à transmission radiofréquence, qui utilisent une clé électronique ou un badge portatif pour le déverrouillage des portes et des immobiliseurs antivols d'un véhicule automobile.

Les exigences imposées en terme de sécurité aux télécommandes et aux systèmes d'identification à transpondeur pour l'application automobile impliquent des méthodes de transmission des données entre la télécommande ou le transpondeur d'une part, et le véhicule d'autre part, qui soient suffisamment élaborées pour rendre inefficace l'enregistrement des communications à des fins de création de télécommandes ou de transpondeurs pirates, même pour un malfaiteur ayant momentanément accès au véhicule et à sa clé.

Dans l'art antérieur, les méthodes de transmission qui sont utilisées, notamment pour la communication avec les transpondeurs auto-alimentés tels que des badges d'identification, font appel à des techniques d'interrogation et de réponse basées sur l'échange de données. L'utilisation des codes évolutifs pour le cryptage des données à transmettre impose que ces codes évolutifs soient périodiquement mémorisés en mémoire volatile afin d'empêcher toute recopie frauduleuse des messages transmis pouvant servir à l'établissement de clés pirates.

Dans ce type de transmission à codage évolutif, la clé à transpondeur doit comporter des moyens pour permettre l'écriture de la nouvelle valeur des codes

évolutifs à chaque séquence d'identification et de commande. Ces moyens sont généralement constitués par une mémoire non volatile. Ce type de transmission à codage évolutif est bien adapté aux transpondeurs auto-alimentés tels que des badges d'identification.

Il comporte cependant des risques de perte de la synchronisation entre le transpondeur et le module d'interrogation, rendant impossible toute utilisation de la clé à transpondeur sauf à enclencher une pahse d'apprentissage.

De plus ce type de transmission à codage évolutif est particulièrement mal adapté aux systèmes utilisant des transpondeurs passifs téléalimentés miniature.

En effet dans ce type de transmission, la sauvegarde des codes évolutifs exige dans le transpondeur un surcroît d'énergie consommée au moment de l'écriture dans la mémoire.

Ceci est particulièrement pénalisant pour les transpondeurs passifs miniatures du type téléalimentés par couplage magnétique, qui ne disposent que de très peu d'énergie pour la sauvegarde des données en mémoire non volatile.

Par ailleurs, la multiplication des temps nécessaires à chaque phase d'identification, induite par la préparation de la communication suivante, est un critère limitatif des procédés de transmission de l'état de la technique.

En effet, dans l'application destinée au déverrouillage des portes et des immobiliseurs antivols d'un véhicule, en particulier lors de l'action de démarrage du moteur, l'identification de la clé (ou du badge) à transpondeur doit être réalisée dans un temps relativement court afin de rendre l'opération imperceptible au conducteur.

Afin d'éliminer les inconvénients de l'état de la technique précités, la présente invention dispose un procédé d'identification d'une clé ou d'un badge à transpondeur téléalimenté qui soit simple et fiable, et dans lequel une seule phase d'interrogation et de réponse du transpondeur n'est requise.

En effet, la présente invention concerne un procédé de communication entre un module d'interrogation et une clé à transpondeur, utilisé en particulier pour le déverrouillage des ouvrants et/ou des immobiliseurs d'un véhicule automobile, du type comportant notamment une séquence de réveil du module d'interrogation, une séquence d'identification consistant à interroger la clé à transpondeur en émettant au moins un signal d'interrogation et à vérifier la validité de la réponse de la clé transpondeur, et une séquence d'activation des moyens de déverrouillage des ouvrants et/ou des immobiliseurs, caractérisé en ce que la séquence d'identification ne comporte qu'une seule étape d'émission d'un message d'interrogation et une seule étape de réception d'un message de réponse de la clé à transpondeur.

L'avantage de ce procédé de communication réside dans le fait qu'il ne comporte aucune étape d'écriture de données dans une mémoire non volatile, éliminant ainsi la nécessité d'utiliser de telles mémoires, comme des mémoires en technologie EEPROM.

Cette caractéristique se traduit, par un coût, du système d'identification qui est divisé par deux, une meilleure fiabilité, une plus grande longévité et une taille réduite pour la clé à transpondeur.

Par ailleurs, un autre avantage du procédé de communication selon l'invention réside dans le fait que le module d'interrogation vérifie la validité du code de

la clé à transpondeur sans que celui-ci soit jamais transmis.

En effet, lors de la séquence d'identification, seule une image du code de la clé à transpondeur est transmise.

Dans le procédé de communication selon l'invention la séquence d'identification comporte en outre :

- une étape où le module d'interrogation génère un code aléatoire CAi ;
- une étape où le module d'interrogation procède à la formation du message d'interrogation à partir du code aléatoire CAi ;
- une étape où le transpondeur reçoit le message d'interrogation;
- une étape où le transpondeur procède au calcul du code de réponse CRTi;
- une étape où le transpondeur procède à la formation du message de réponse à partir du code de réponse CRTi ;
- une étape où le transpondeur procède à la transmission du message de réponse;
- une étape où le module d'interrogation procède au calcul du code de réponse attendu CRMi ;
- une étape où le module d'interrogation reçoit le message de réponse;
- une étape où le module d'interrogation procède à la comparaison entre le code de réponse CRTi, extrait du message de réponse reçu, et le code de réponse attendu CRMi.

Selon un autre aspect de l'invention, l'étape où le module d'interrogation procède à la comparaison entre le code de réponse et le code de réponse attendu, est suivie:

- soit d'une étape concluant à l'identification de la clé à transpondeur, si le code de réponse du transpondeur et le code de réponse attendu sont égaux ;

- soit d'une étape concluant à la non identification de la clé à transpondeur, si le code de réponse et le code de réponse attendu sont différents.

Selon un autre aspect de l'invention, lors de l'étape où le transpondeur calcule le code de réponse CRTi, un processeur effectue le calcul à partir :

- du code aléatoire CAi extrait du message d'interrogation reçu;

- d'une fonction de cryptage f prédéterminée;

- d'au moins une clé de cryptage Kt prédéterminée,

suivant la formule CRTi=f(CAi, Kt).

Selon un autre aspect de l'invention, lors de l'étape où le module d'interrogation procède au calcul du code de réponse attendu CRMi, un processeur effectue le calcul à partir :

- du code aléatoire CAi;

- de la fonction de cryptage f prédéterminée;

- d'au moins une clé de cryptage Km prédéterminée,

suivant la formule CRMi=f(CAi, Km).

Selon un autre aspect de l'invention, la fonction de cryptage f est une donnée propre au couple module d'interrogation / clé à transpondeur

Selon un autre aspect de l'invention, la fonction de cryptage f est une fonction injective c'est à dire qu'à une valeur CAi donnée donnée, ne correspond qu'un seul couple de valeurs (Kt, CRTi) [respectivement (Km, CRMi)].

Selon un autre aspect de l'invention, la fonction de cryptage f est réalisée par des opérations logiques élémentaires telles que, de manière non limitative, le OU

exclusif, l'addition binaire, le décalage binaire, le test des valeurs des éléments binaires.

Selon un autre aspect de l'invention, le code aléatoire CAi, et les clés de cryptage Kt et Km sont des nombres binaires dont la taille est comprise entre 40 et 64 bits.

Par ailleurs, l'invention concerne aussi un dispositif d'identification pour un système de déverrouillage des ouvrants et/ou des immobiliseurs d'un véhicule, du type comportant :

- un module d'interrogation;
- au moins une clé ou un badge à transpondeur;
- des moyens de réveil du module d'interrogation, adaptés à déclencher la séquence d'identification;
- des moyens de déverrouillage des ouvrants et des immobiliseurs antivols du véhicule,

caractérisé en ce qu'il met en oeuvre un procédé de communication tel que celui décrit ci-dessus.

Selon un autre aspect de l'invention, le transpondeur est du type ne comportant pas de mémoire non volatile.

Selon un autre aspect de l'invention, le véhicule et la clé à transpondeur comportent chacun des moyens tels qu'une antenne basse fréquence pour émettre respectivement le message d'interrogation et le message de réponse sous la forme d'une onde radioélectrique à porteuse modulée basse fréquence, comprise entre 80 et 150 Khz, et des moyens de réception équivalents.

La méthode de transmission des données du système d'identification qui met en oeuvre le procédé d'identification de l'invention rend pratiquement impossible la copie de la clé, même lorsqu'un malfaiteur a momentanément accès au véhicule et à sa clé.

De plus le niveau de sécurité du système d'identification n'est pas réduit lorsque tous les détails de la réalisation du système sont connus.

Enfin, les temps de communication pour l'identification de la clé du véhicule restent inférieurs à 200ms, ce qui est une excellente performance pour un système ayant un tel degré de sécurité bien que fonctionnant à une fréquence comprise entre 80 et 150 Khz.

D'autres caractéristiques et avantages de la présente invention seront mieux compris à la lecture de la description qui va suivre en référence aux dessins annexés qui sont :

- la figure 1 : un schéma d'un dispositif d'accès par clé à transpondeur appliqué au déverrouillage des ouvrants et/ou des immobiliseurs d'un véhicule ;
- la figure 2 : un schéma illustrant une méthode de transmission pour l'identification de la clé à transpondeur d'un véhicule selon un principe connu dans l'état de la technique ;
- la figure 3 : un schéma illustrant le procédé de transmission pour l'identification de la clé à transpondeur d'un véhicule selon l'invention ;
- la figure 4 : un schéma du principe de fonctionnement du système d'identification selon l'invention ;
- la figure 5 : un mode de réalisation d'une clé à transpondeur selon l'invention.

A la figure 1, on a représenté un schéma de principe d'un dispositif d'accès par clé ou badge à transpondeur. Le véhicule 11 comporte un module d'interrogation qui, sous certaines conditions, produit un message d'interrogation 12 vers un badge à transpondeur 13 qui produit en retour un message de réponse 14. Les messages d'interrogation et de réponse

sont transmis sous la forme d'une onde radiofréquence dans la gamme 80 Khz - 5 MHz.

Dans le mode de fonctionnement de l'invention, l'utilisateur active les moyens de réveil du module d'interrogation, ce qui déclenche l'émission du message d'interrogation 12 par exemple en manipulant la poignée 15 de la portière 16 du conducteur. La poignée comporte un détecteur de manipulation constitué notamment par un interrupteur à levier solidaire de la poignée mobile de porte, dont le signal de sortie est transmis par une liaison filiaire ou autre au module de bord 17 qui produit alors le message d'interrogation à l'aide d'antennes disposées à la périphérie du véhicule, par exemple une antenne BF dans un rétroviseur extérieur 19.

Si le badge 13 est dans la portée de transmission de l'antenne BF, il répond au module de bord 17 par un message de réponse 14. Si le module de bord 17 identifie le badge 13 comme un badge autorisé, il active le déverrouillage des portes.

Dans un mode de réalisation préféré, représenté à la figure 5, l'utilisateur active les moyens de réveil du module d'interrogation, en insérant une clé à transpondeur dans le cylindre de l'antivol de direction et en la positionnant sur la position de démarrage.

A la figure 2, on a représenté un schéma illustrant un procédé de transmission pour l'identification de la clé d'un véhicule selon un principe connu dans l'état de la technique.

Les étapes de ce procédé classique de l'art antérieur sont représentées l'une en dessous des autres, avec, en colonne avec sur la partie gauche de la figure, celles qui sont effectuées par le module d'interrogation, et, en colonne sur la partie droite, celles qui sont effectuées par le transpondeur.

Ces deux colonnes sont séparées par une droite verticale 200 qui représente le milieu de propagation séparant le module d'interrogation et la clé à transpondeur, et à travers lequel les émissions sont faite dans un sens ou dans l'autre.

La transmission est divisée en un certain nombre d'étapes que l'on peut classiquement regrouper suivant deux séquences principales :

- une première séquence, dite séquence d'identification, dont le but est de permettre au module d'interrogation et à la clé à transpondeur de se reconnaître mutuellement ;

- une deuxième séquence, dite séquence de changement de code de la clé à transpondeur, qui est destinée à modifier le code de façon bilatérale afin que, lors de l'identification suivante, celui-ci soit différent de sa valeur courante.

La séquence d'identification démarre lorsqu'une clé à transpondeur est présentée. Le module d'interrogation transmet, lors d'une étape 202, un message d'interrogation contenant un mot de passe MP préprogrammé à la fois dans le module de bord et dans le transpondeur, et ce lors d'une phase d'appairage en usine.

Après la réception 201 du message d'interrogation, le transpondeur de la clé vérifie par un test 203 que le mot de passe MP reçu correspond à un mot de passe de référence mémorisé:

- si tel est le cas, le transpondeur de la clé effectue la transmission 205 d'un message de réponse Ri contenant un code clé Ci contenu en mémoire ;

- sinon, le transpondeur ne reconnaît pas le module d'interrogation et la séquence d'identification s'achève là.

Dans le premier cas, et lorsque le code clé Ci est validé par un test 204 effectué par le module d'interrogation, l'identification est validée, la séquence d'identification se termine avec succès, et le module d'interrogation transmet une commande de déverrouillage aux dispositifs de fermeture et à l'immobiliseur antivol du véhicule.

Ensuite commence la deuxième séquence, qui consiste tout d'abord à transmettre au transpondeur de la clé un nouveau code clé Ci+1 qu'il lui faudra utiliser lors de la prochaine séquence d'identification.

Le module d'interrogation crée d'abord un nouveau code clé Ci+1 par un processus 206 de génération de valeurs aléatoires ou pseudoaléatoires. Il transmet ensuite dans un message de programmation Pi ce nouveau code clé Ci+1 au transpondeur de la clé du véhicule en utilisant une nouvelle fois le mot de passe MP.

Après avoir reçu ce message de programmation Pi et après avoir vérifié de nouveau la validité du mot de passe MP, le transpondeur de la clé sauvegarde ce nouveau code clé Ci+1 en, en écrasant l'ancien code clé Ci, et transmet un accusé de réception au module d'interrogation. A réception 208 de cet accusé de réception, le module d'interrogation sauvegarde le nouveau code clé Ci+1 en mémoire.

Ce nouveau code clé Ci+1 devient pour le module d'interrogation le nouveau code clé de référence attendu lors de la prochaine séquence d'identification.

On voit que ce type de procédé nécessite d'utiliser des mémoires non volatiles et reprogrammables, du type d'une mémoire en technologie EEPROM par exemple. Le processus d'écriture dans ces mémoires est un processus qui requiert un surplus de consommation d'énergie qui est particulièrement pénalisant pour un transpondeur du type téléalimenté par couplage inductif.

Par ailleurs, la répétition des échanges se traduit par un allongement de la durée totale de l'opération de déverrouillage. En effet, au moins deux interrogations et deux réponses du transpondeur sont requises. Or compte tenu des limites imposées par l'intégration des antennes d'émission et de réception dans le transpondeur, qui sont des limites d'espace notamment, on est obligé de fonctionner à des fréquences relativement basses, limitant ainsi la bande passante disponible. La vitesse de transmission des informations binaires est donc limitée et un procédé tel que celui décrit ci-dessus ne peut remplir les objectifs de rapidité de l'identification qui sont requis dans notre application.

A la figure 3 le procédé de transmission pour l'identification selon le principe de l'invention est présenté de la même façon que le procédé de l'état de la technique décrit à la figure 2.

Le procédé d'identification débute par une étape 302 destinée à la génération par le module de bord d'un code aléatoire ou pseudoaléatoire CAi. Ce code est généré selon toute méthode connue de l'Homme du Métier, comme par exemple à l'aide d'un compteur rebouclé dont la période est très inférieure à celle d'un phénomène extérieur utilisé pour interrompre le comptage sur une valeur donnée, cette valeur pouvant donc être considérée comme pseudoaléatoire.

De la longueur de ce code dépendra le niveau de sécurité de la transmission, car plus le code peut prendre de valeurs différentes et plus le système sera efficace en terme de sécurité des transmissions. Un code de 40 à 64 bits est considéré comme produisant un niveau de sécurité suffisant pour notre application.

Dans une étape 304, le module d'interrogation forme ensuite un message d'interrogation Mi qui comporte

notamment le code aléatoire CAi ainsi que des bits de contrôle destinés à imposer un format spécifique au message Mi afin de faciliter son acquisition et son exploitation par le tranpondeur. Ces bits peuvent par exemple contenir des informations de début de trame, de fin de trame, de parité, etc...

Lors d'une étape 306 le message d'interrogation est émis sur une antenne d'émission radiofréquence ainsi qu'il a été vu à la figure 1.

Le message d'interrogation Mi est capté par le transpondeur, placé dans le champ d'émission de l'antenne, ce qui constitue une étape 301 qui est la première étape où celui-ci intervient.

Après avoir reçu le message d'interrogation Mi, le transpondeur en extrait le code aléatoire CAi et opère le calcul 303 de la réponse en procédant à la génération d'un code, dit code de la réponse du transpondeur CRTi, à l'aide d'une fonction de cryptage déterminée f qui, en outre, utilise au moins une clé de cryptage Kt. Le code CRTi est ainsi défini par la relation CRTi=f(CAi,Kt).

La clé de cryptage Kt constitue une donnée propre à la clé à transpondeur considérée.

Le calcul du code de réponse du transpondeur CRTi est effectué par un processeur, par exemple un microcontrôleur ou un ASIC, contenu dans la clé à transpondeur.

Parallèlement, après avoir émis le message d'interrogation Mi, le module d'interrogation opère le calcul 308 de la réponse que doit lui faire le transpondeur autorisé, en procédant à la génération d'un code, dit code de réponse attendu par le module CRMi, à l'aide de la même fonction de cryptage déterminée f que celle utilisée par le transpondeur et qui, en outre, utilise au moins une clé de cryptage Km. Le code CRMi est ainsi défini par la relation CRMi=f(CAi,Km).

La clé de cryptage Km constitue une donnée propre au module d'interrogation considéré, et représente le code de la clé autorisée à déverrouiller les ouvrants du véhicule.

Le calcul du code de réponse attendu par le module CRMi est effectué par un processeur, par exemple un microcontrôleur ou un ASIC, contenu dans le module d'interrogation.

La fonction f est une donnée propre au couple module d'interrogation / clé à transpondeur. Les clés de cryptage Kt et Km sont créées par un processus de génération de code aléatoire, lors d'une opération d'appairage réalisée avant ou pendant l'installation du systeme dans le véhicule.

La fonction de cryptage f peut être considérée comme une fonction de la variable CAi et dont la clé de cryptage Kt (ou Km) est un paramètre, et est une fonction particulière dont les propriétés sont les suivantes :

- elle est injective, c'est à dire qu'à une valeur CAi donnée donnée, ne correspond qu'un seul couple de valeurs (Kt, CRTi) [respectivement (Km, CRMi)] ;
- elle n'est pas inversible, c'est à dire qu'il n'existe pas de fonction analytique g telle que g(Kt, CRTi)=CAi [respectivement g(Km, CRMi)=CAi] ;
- elle fait appel à des opérations logiques élémentaires telles que le OU Exclusif, le décalage binaire, l'addition binaire, le test des valeurs des éléments binaires, etc... Ces opérations sont facilement éxécutables par un microprocesseur de faible puissance de calcul ou par un circuit intégré spécifique.

Dans un mode de réalisation préféré de l'invention, la taille des clés de cryptage Kt,Km est comprise entre 40 et 64 bits, ce qui permet d'obtenir un niveau de sécurité optimum.

Après avoir calculé le code de réponse CRTi, le transpondeur enchaîne sur une étape 305 de formation du message de la réponse Ri, similaire à l'étape 304 de formation du message de l'interrogation décrite précedemment. Dans le même temps, le module d'interrogation reste inactif et dans une étape 310 d'attente de la réponse.

Le transpondeur émet ensuite le message de réponse Ri lors d'une étape 309, et le module d'interrogation le reçoit lors d'une étape 312.

Le rôle joué par le transpondeur dans le procédé d'identification est alors terminé. Il reste au module d'interrogation à extraire le code de réponse du transpondeur CRTi du message de réponse Ri reçu, et à le comparer au code de réponse attendue CRMi lors d'une étape 314.

- si le code de réponse du transpondeur CRTi et le code de réponse attendu par le module d'interrogation CRMi sont égaux, et compte tenu de la propriété d'injectivité de la fonction f, cela signifie que la clé de cryptage Kt du transpondeur et la clé de cryptage Km du module d'interrogation sont égales. Le module d'interrogation conclut alors à l'identification de la clé à transpondeur ce qui constitue une fin possible 316 pour le procédé ;

- dans le cas contraire, c'est-à-dire si le code CRMi est différent du code CRTi, c'est-à-dire aussi si la clé de cryptage Kt du transpondeur et la clé de cryptage km du module d'interrogation sont différentes, le module d'interrogation conclut à la non identification de la clé à transpondeur, ce qui constitue une autre fin possible 318 du procédé d'identification.

On voit que le procédé d'identification de l'invention ne nécessite qu'une étape d'interrogation et qu'une étape de réponse de la clé à transpondeur.

Pour un transpondeur téléalimenté miniature fonctionnant sur le principe du couplage magnétique à une fréquence comprise entre 80 Khz et 5 MHz, les temps de communication pour l'identification restent inférieurs à 200ms, ce qui est pratiquement imperceptible pour l'utilisateur.

Par ailleurs, on démontre par des analyses et des calculs mathématiques ainsi qu'avec des simulations à l'aide d'un ordinateur, qu'il n'exite pas de moyen simple pour calculer la clé de cryptage Kt à partir d'un ou de plusieurs couples de valeurs (CAi, CRTi), même lorsque la fonction de cryptage f est connue.

L'interrogation de la clé par un module pirate, et l'enregistrement des réponses de la clé transpondeur à plusieurs interrogations successives, ne permet donc pas de retrouver facilement la clé de cryptage Kt.

En fait, la seule méthode connue qui permettrait de retrouver la clé de cryptage Kt serait de tester systématiquement toutes les valeurs possibles de la clé de cryptage Kt dans un processus de calcul qui intègrerait la fonction f. Compte tenu du nombre de valeurs possibles que peut prendre la clé Kt, les temps de calcul, même avec un ordinateur puissant, sont très persuasifs. En effet, en considérant un code de clé Kt de 48 bits, on obtient un nombre de valeurs du code de clé égal à 2^{48}. En supposant un temps de calcul élémentaire pour un test d'une valeur de clé Kt égal à 1μs, on obtient un temps de calcul de 8 ans pour effectuer un balayage systématique de toutes les valeurs de code de la clé kt.

Le procédé d'identification décrit ci-dessus est une version simplifiée de l'invention. Des variantes sont possibles dans lesquelles un module d'interrogation peut identifier plusieurs clés à transpondeur différentes,

afin par exemple de permettre l'accès au véhicule par plusieurs personnes autorisées différentes.

Dans ce cas, l'étape 308 de la figure 3 est multipliée autant de fois qu'il y a de clés en service, celles-ci ayant toutes un code de clé différent afin d'identifier un utilisateur autorisé d'un autre, et de permettre par exemple d'actionner un dispositif de réglage automatique de la position des sièges ou des rétroviseurs sur une position déterminée et personnalisée.

Le module de bord dispose alors d'une pluralité de code de clé Kmj en mémoire et l'étape 308 est renouvelée pour chacun de ces codes de clé Kmj, les résultats CRMij étants tous sauvegardés en mémoire et comparés au code de réponse du transpondeur CRTi.

- si le code de réponse du transpondeur CRTi et l'un des codes de réponse attendus par le module d'interrogation CRMij sont égaux, c'est que les clés de cryptage du transpondeur Kt et du module d'interrogation Kmj sont égales. Le module d'interrogation conclut alors à l'identification de la clé ;

- dans le cas contraire, c'est à dire si aucun des codes CRMij n'est égal au code CRTi le module d'interrogation conclut à la non identification de la clé.

Par ailleurs, plusieurs modules d'interrogation installés sur des véhicules différents peuvent admettre la même clé, ce qui permet à un même utilisateur d'accéder à plusieurs véhicules avec une clé unique.

A la figure 4, le dipositif de verrouillage selon l'invention comporte un module d'interrogation 47 et un transpondeur 43 qui utilisent le procédé d'identification décrit ci-dessus.

Des moyens de réveil 41 permettent de déclencher la séquence d'identification, qui, comme il a été

présenté, est notamment constituée par une émission unique d'un message d'interrogation 42 par des moyens d'émission du module d'interrogation, et par l'émission unique d'un message de réponse 44 par des moyens d'émission du transpondeur 43.

Ces moyens de réveil 41 sont par exemple réalisés par un détecteur de manipulation sous une poignée de portière, par exemple sous la poignée de la portière du conducteur, ainsi qu'il a été décrit à l'aide de la figure 1, ou par une position déterminée, comme la position de démarrage de la clé à transpondeur que l'on insère dans le cylindre antivol du véhicule. Ces moyens de réveil 41 peuvent ainsi être constitués par un bouton de démarrage disposé à cet effet par exemple sur le tableau de bord.

Le dispositif comporte par ailleurs des moyens 49 de déverrouillage des ouvrants et des immobiliseurs du véhicule. Ces moyens sont reliés, par exemple, aux dispositifs de condamnation des portières et aux dispositifs antivols du véhicule.

A la figure 5, on a représenté un mode de réalisation d'une clé à transpondeur selon l'invention. La clé 50 comporte une première partie ou insert de clé 53, destinée à être insérée dans le cylindre d'antivol 52 du véhicule, et une seconde partie ou tête de clé 51 qui reste à l'extérieur. Dans la tête de clé 51 est disposé un transpondeur 55 de diamètre D.

L'insert de clé 53 comporte des moyens, tels que des crans, qui permettent l'insertion de la clé 50 dans le cylindre d'antivol 52 et qui permettent de tourner celui-ci dans une position dite position de démarrage. Lorsque le cylindre d'antivol est placé dans cette position de démarrage, le module d'interrogation [illegible]

représenté) est réveillé et émet un signal d'interrogation par l'intermédiaire d'un moyen rayonnant tel qu'une antenne 56.

Cette antenne 56 est ramenée à la périphérie extérieure du cylindre d'antivol, c'est à dire à proximité de la zone où se trouve le transpondeur 55 lorsque la clé 50 est insérée et tournée en position de démarrage.

Le transpondeur 55 est un transpondeur passif téléalimenté miniature. Il tire son alimentation par induction magnétique selon une méthode connue dans l'état de la technique. En effet, le module d'interrogation rayonne par son antenne 56 de l'énergie électromagnétique à une fréquence déterminée, et ce pendant toute la durée de l'identification ou pendant une partie de la phase d'identification, le transpondeur comportant des moyens pour récupérer cette énergie pour son alimentation propre.

La quantité d'énergie Er reçue par le transpondeur 55 est une fonction décroissante de la distance d qui sépare l'antenne 56 transpondeur 55. Elle est par ailleurs une fonction croissante du diamètre D du transpondeur, puisque croissante du diamètre de l'antenne dudit transpondeur. Enfin la quantité d'énergie Er reçue par le transpondeur est une fonction croissante avec la quantité d'énergie émise Ee par le module d'interrogation.

Ce qui précède peut se résumer par la formule $Er = g(d, D, Ee)$ où g est une fonction qui tient compte des pertes diverses du couplage inductif, en particulier [illegible]

pertes magnétiques dans les masses métalliques de l'antivol de direction.

Dans la pratique, il existe une distance minimale, imposée par les contraintes d'exploitation en dessous de laquelle la distance d qui sépare l'antenne 56 du module d'interrogation et le transpondeur ne peut descendre. Par ailleurs, le diamètre D du transpondeur 55 ne peut dépasser une valeur maximale imposée par l'épaisseur de la clé.

Par conséquent, l'énergie que capte le transpondeur est une énergie précieuse. Le procédé d'identification selon l'invention permet d'économiser une grande part de cette énergie puisqu'il ne nécessite pas d'écrire dans une mémoire non volatile du transpondeur telle qu'une mémoire en technologie EEPROM, opération qui est est gourmande en énergie.

Ainsi, le procédé d'identification selon l'invention permet de créer des dispositifs d'identification avec une distance d qui sépare l'antenne du module d'interrogation et le transpondeur plus importante, et une énergie Ee à émettre sur l'antenne 56 du transpondeur plus faible.

Cet avantage s'ajoute au fait qu'un transpondeur qui ne nécessite pas de puce EEPROM de mémoire non volatile est un transpondeur qui coûte beaucoup moins cher qu'un transpondeur qui en comporte une. De plus, un transpondeur sans puce EEPROM autorise un nombre d'utilisations quasiment illimité, du moins non limité par la cause principale d'usure des transpondeurs classiques de l'état de la technique, qui est [illegible]

nombreuses réécritures que subit la mémoire non volatile qu'ils comportent.

REVENDICATIONS

1- Procédé de communication entre un module d'interrogation et une clé transpondeur, utilisé en particulier pour le déverrouillage des ouvrants et/ou des immobiliseurs d'un véhicule automobile, du type comportant notamment une séquence de réveil du module d'interrogation, une séquence d'identification consistant à interroger la clé en émettant au moins un signal d'interrogation et à vérifier la validité de la réponse de la clé transpondeur, et une séquence d'activation des moyens de déverrouillage des ouvrants et/ou des immobiliseurs, caractérisé en ce que la séquence d'identification ne comporte qu'une seule étape d'émission (306) d'un message d'interrogation (Mi) et une seule étape de réception (312) d'un message de réponse (Ri) de la clé transpondeur.

2- Procédé de communication selon la revendication 1, caractérisé en ce que la séquence d'identification comporte en outre :

- une étape (302) où le module d'interrogation (7) génère un code aléatoire (CAi);
- une étape (304) où le module d'interrogation (7) procède à la formation d'un message d'interrogation (Mi) à partir du code aléatoire CAi ;
- une étape (301) où le transpondeur (13) reçoit le message d'interrogation (Mi);
- une étape (303) où le transpondeur (13) procède au calcul d'un code de réponse CRTi;
- une étape (305) où le transpondeur (13) procède à la formation d'un message de réponse (Ri) à partir du code de réponse CRTi ;
- une étape (309) où le transpondeur (13) procède à transmission du message de réponse (Ri);

- une étape (308) où le module d'interrogation (7) procède au calcul d'un code de réponse attendu CRMi;
- une étape (312) où le module d'interrogation (7) reçoit le message de réponse (Ri);
- une étape (314) où le module d'interrogation (7) procède à la comparaison entre le code de réponse CRTi extrait du message de réponse (Ri) reçu et le code de réponse attendu CRMi;

3- Procédé de communication selon la revendication 2, caractérisé en ce ce que l'étape (314) où le module d'interrogation (7) procède à la comparaison entre le code de réponse (CRTi) et le code de réponse attendu (CRMi), est suivie :

- soit d'une étape (316) concluant à l'identification de la clé à transpondeur, si le code de réponse du transpondeur (CRTi) et le code de réponse attendu (CRTi) sont égaux ;
- soit d'une étape (318) concluant à la non identification de la clé à transpondeur si le code de réponse (CRTi) et le code de réponse attendu (CRTi) sont différents.

4- Procédé de communication selon la revendication 2, caractérisé en ce ce que lors de l'étape (301) où le transpondeur (13) calcule le code de réponse CRTi, un processeur effectue le calcul à partir :

- du code aléatoire CAi extrait du message d'interrogation (Mi) reçu;
- d'une fonction de cryptage f prédéterminée;
- d'au moins une clé de cryptage Kt prédéterminée,

suivant la formule CRTi=f(CAi, Kt).

5- Procédé de communication selon les revendication 2 et 4, caractérisé en ce ce que lors de l'étape (308) où le module d'interrogation (13) procède au calcul du code de réponse attendu CRMi, un processeur effectue le calcul à partir :

- du code aléatoire CAi;
- de la fonction de cryptage f prédéterminée;
- d'au moins une clé de cryptage Km prédéterminée,

suivant la formule CRMi=f(CAi, Km).

6- Procédé de communication selon la revendication 4 et la revendication 5, caractérisé en ce que la fonction de cryptage f est une donnée propre au couple module d'interrogation / clé à transpondeur.

7- Procédé de communication selon la revendication 4 et la revendication 5, caractérisé en ce que la fonction de cryptage f est une fonction injective c'est à dire qu'à une valeur CAi donnée donnée, ne correspond qu'un seul couple de valeurs (Kt, CRTi) [respectivement (Km, CRMi)].

8- Procédé de communication selon l'une quelconque des revendication 4 à 7, caractérisé en ce que la fonction de cryptage f est réalisée par des opérations logiques élémentaires telles que, de manière non limitative, le OU exclusif, l'addition binaire, le décalage binaire, le test des valeurs des éléments binaires.

9- Procédé de communication selon la revendication 4 et la revendication 5, caractérisé en ce que le code aléatoire CAi, et les clés de cryptage Kt et

Km sont des nombres binaires dont la taille est comprise entre 40 et 64 bits.

10- Dispositif d'identification pour un système de déverrouillage des ouvrants et/ou des immobiliseurs d'un véhicule, du type comportant :

- un module d'interrogation (17);
- au moins une clé ou un badge à transpondeur (13);
- des moyens (41) de réveil du module d'interrogation, adaptés à déclencher la séquence d'identification;
- des moyens (49) de déverrouillage des ouvrants et des immobiliseurs antivols du véhicule,

caractérisé en ce qu'il met en oeuvre un procédé de communication selon l'une quelconque des revendications précédentes.

11- Dispositif selon la revendication 10, caractérisé en ce que le transpondeur (13) est du type ne comportant pas de mémoire non volatile.

12- Dispositif selon la revendication 10 ou la revendication 11, caractérisé en ce que le véhicule (11) et la clé à transpondeur (13) comportent chacun des moyens tels qu'une antenne pour émettre respectivement le message d'interrogation (Mi) et le message de réponse (Ri) sous la forme d'une onde radioélectrique à porteuse modulée et des moyens de réception équivalents.

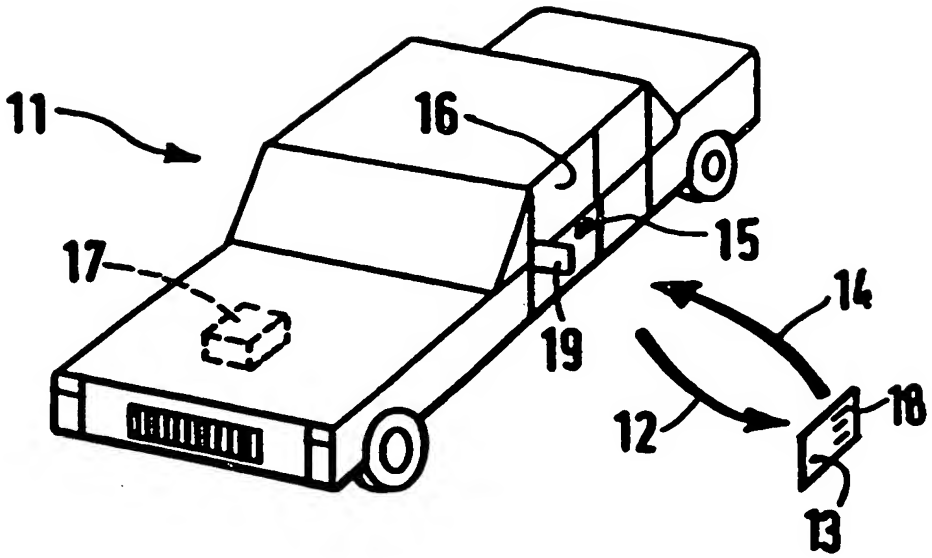


FIG.1

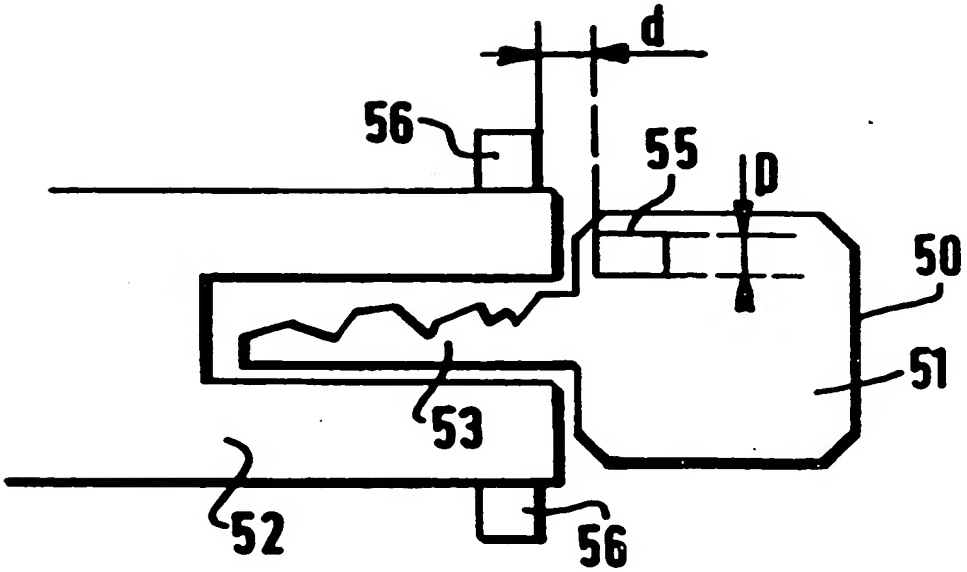


FIG.5

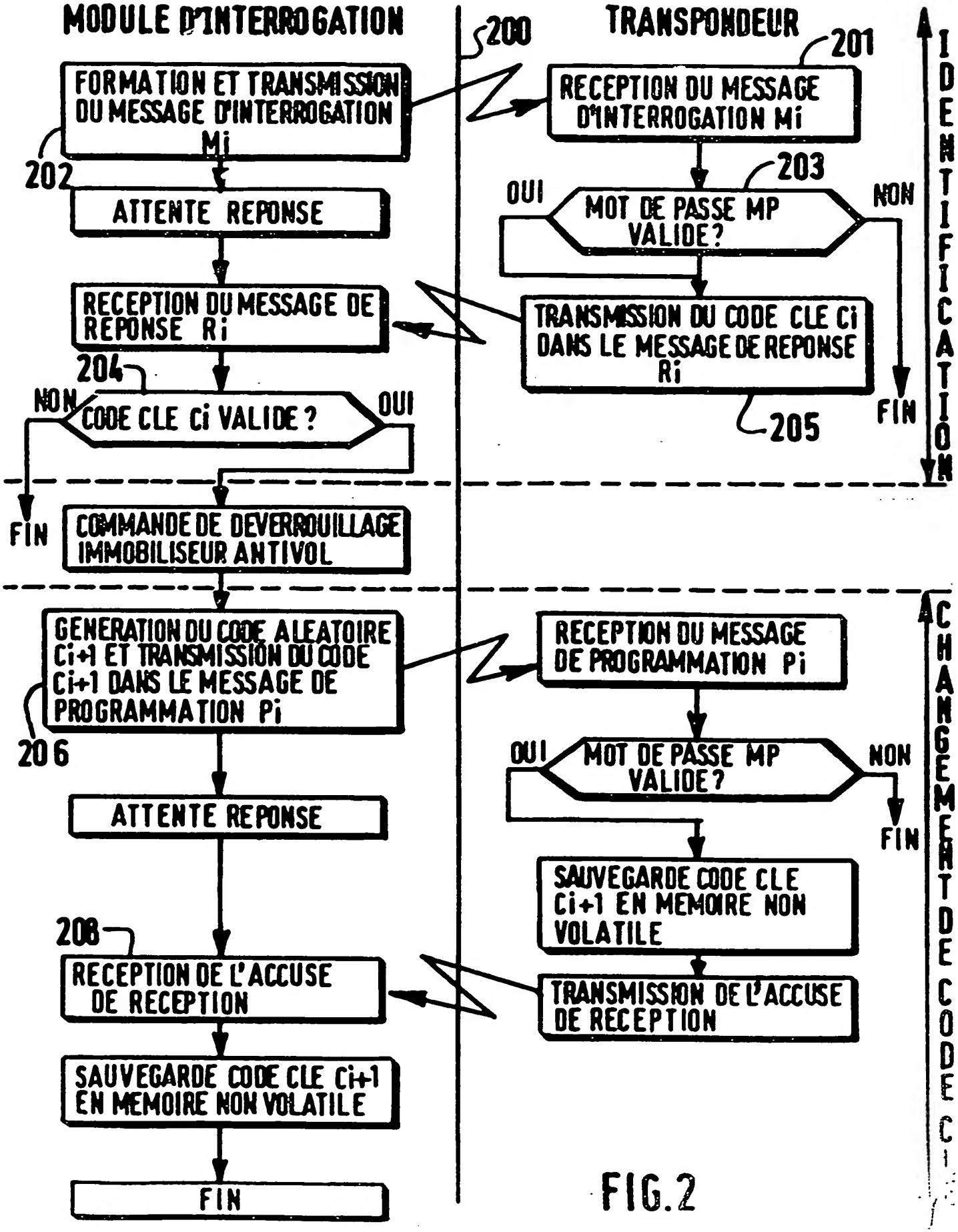

MODULE D'INTERROGATION
TRANSPONDEUR
200
201
FORMATION ET TRANSMISSION DU MESSAGE D'INTERROGATION Mi
RECEPTION DU MESSAGE D'INTERROGATION Mi
202
203
ATTENTE REPONSE
OUI
MOT DE PASSE MP VALIDE?
NON
RECEPTION DU MESSAGE DE REPONSE Ri
TRANSMISSION DU CODE CLE Ci DANS LE MESSAGE DE REPONSE Ri
204
NON
CODE CLE Ci VALIDE ?
OUI
205
FIN
FIN
IDENTIFICATION
COMMANDE DE DEVERROUILLAGE IMMOBILISEUR ANTIVOL
GENERATION DU CODE ALEATOIRE Ci+1 ET TRANSMISSION DU CODE Ci+1 DANS LE MESSAGE DE PROGRAMMATION Pi
RECEPTION DU MESSAGE DE PROGRAMMATION Pi
206
OUI
MOT DE PASSE MP VALIDE?
NON
ATTENTE REPONSE
FIN
SAUVEGARDE CODE CLE Ci+1 EN MEMOIRE NON VOLATILE
208
RECEPTION DE L'ACCUSE DE RECEPTION
TRANSMISSION DE L'ACCUSE DE RECEPTION
SAUVEGARDE CODE CLE Ci+1 EN MEMOIRE NON VOLATILE
FIN
CHANGEMENT DE CODE Ci

FIG.2

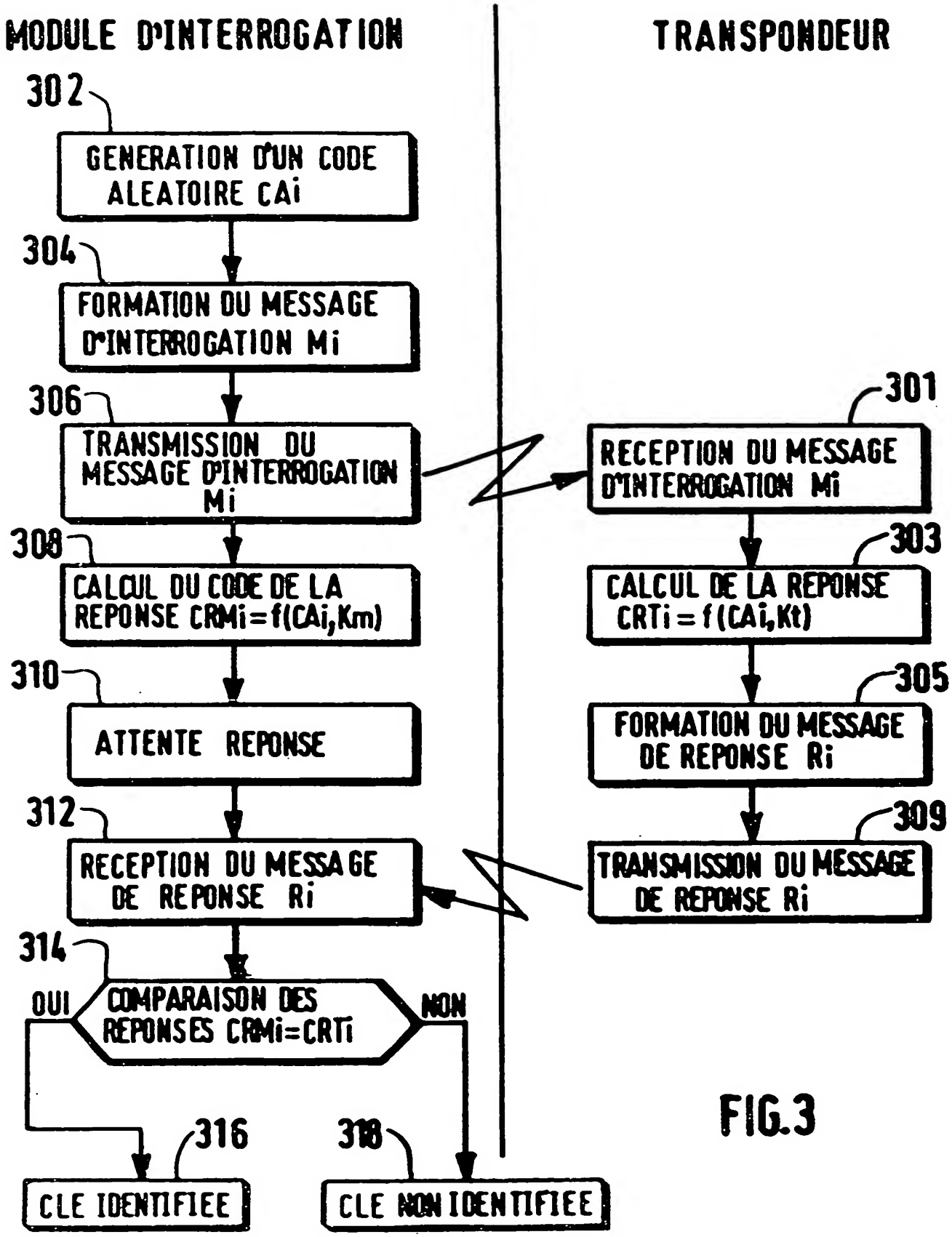

MODULE D'INTERROGATION
TRANSPONDEUR
302
GENERATION D'UN CODE ALEATOIRE CAi
304
FORMATION DU MESSAGE D'INTERROGATION Mi
306
TRANSMISSION DU MESSAGE D'INTERROGATION Mi
308
CALCUL DU CODE DE LA REPONSE CRMi=f(CAi,Km)
310
ATTENTE REPONSE
312
RECEPTION DU MESSAGE DE REPONSE Ri
314
OUI
COMPARAISON DES REPONSES CRMi=CRTi
NON
316
CLE IDENTIFIEE
318
CLE NON IDENTIFIEE
301
RECEPTION DU MESSAGE D'INTERROGATION Mi
303
CALCUL DE LA REPONSE CRTi=f(CAi,Kt)
305
FORMATION DU MESSAGE DE REPONSE Ri
309
TRANSMISSION DU MESSAGE DE REPONSE Ri

FIG.3

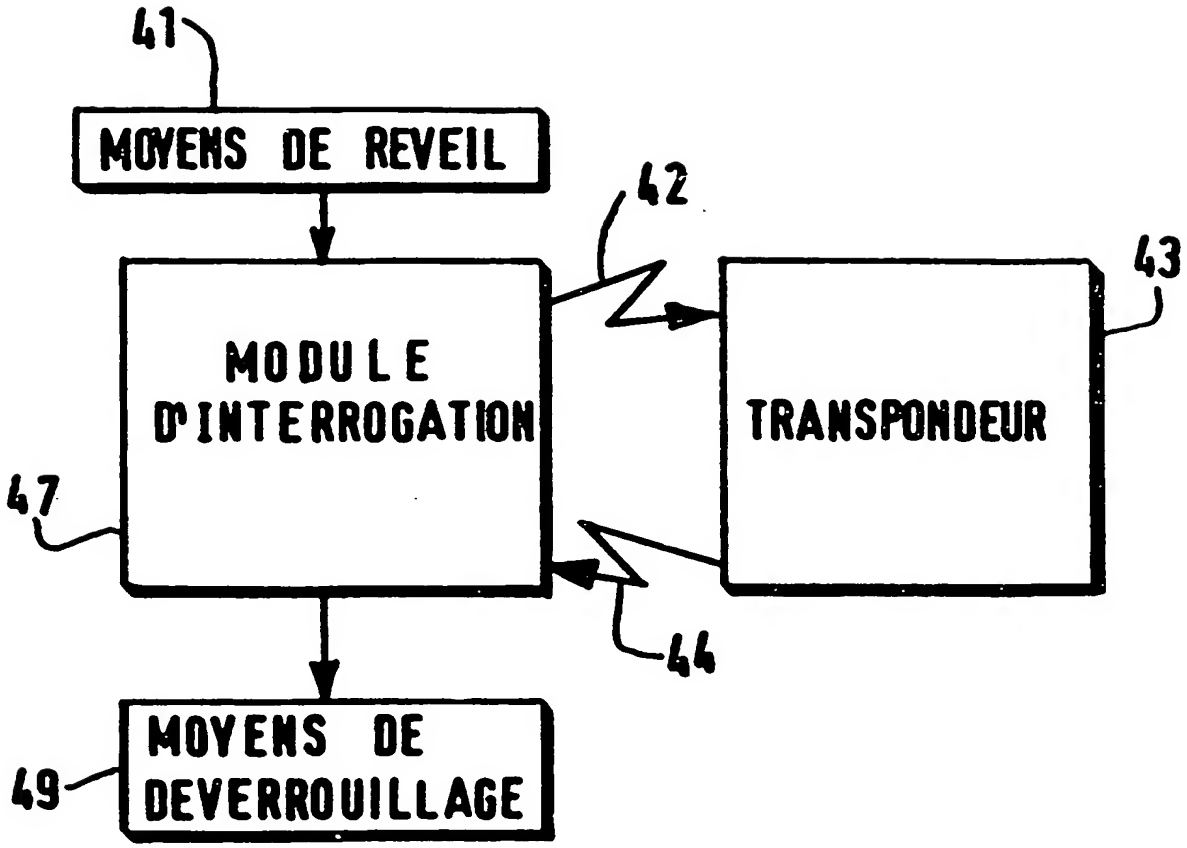

41
MOYENS DE REVEIL
42
43
MODULE D'INTERROGATION
TRANSPONDEUR
47
44
MOYENS DE DEVERROUILLAGE
49

FIG.4

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.